## LISTING OF CLAIMS

IN THE CLAIMS

This listing of the claims is presented without amendment for the convenience of the Examiner:

Claims 1-24 (canceled).

Claim 25 (previously presented): A method for handling encrypted user data objects, the method comprising:

generating a rights object for an encrypted user data object by a data provisioning component, the rights object having assignment information for assigning the rights object to a container object having an encrypted user data object, decryption information for decrypting the encrypted user data object, and rights information for describing usage rights of the encrypted user data object;

generating a confirmation object assigned to the rights object by the data provisioning component, the confirmation object having assignment information for assigning the rights object to an encrypted user data object and a checksum of the encrypted user data object;

transmitting a container object to a first telecommunications device, the container object having a content section in which an encrypted user data object is provided, and a description section in which a determined checksum of the encrypted user data object is provided;

extracting the checksum from the description section of the container object;

re-determining the checksum of the encrypted user data object provided in the content section of the container object;

comparing the extracted checksum with the re-determined checksum so that, should the two checksums tally, an error-free transmission of the encrypted user data object may be concluded;

requesting, via the first telecommunications device, the confirmation object assigned to the rights object to be transmitted to the first telecommunications device;

transmitting the confirmation object from the data provisioning component to the first telecommunications device;

extracting the checksum from the confirmation object; and

comparing the checksum extracted from the confirmation object with the redetermined checksum so that, should the two checksums tally, compatibility of the rights object assigned to the confirmation object and the encrypted user data object transmitted to the first telecommunications device in the container object may be concluded.

Claim 26 (previously presented): A method for handling encrypted user data objects as claimed in claim 25, wherein the data provisioning component provides user data objects which are processed, the processing comprising:

encrypting a user data object provided on the data provisioning component; determining a checksum of the encrypted user data object;

generating a container object having a content section in which the encrypted user data object is provided, and a description section in which the determined checksum of the encrypted user data object is provided; and

transmitting the container object from the data provisioning component to the first telecommunications device.

Claim 27 (previously presented): A method for handling encrypted user data objects as claimed in claim 25, wherein the container object is transmitted to the first telecommunications device by the data provisioning component via at least one further data provisioning component or at least one further telecommunications device.

Claim 28 (previously presented): A method for handling encrypted user data objects as claimed in claim 25, further comprising submitting a request, via the first telecommunications device, to transmit the rights object generated by the data provisioning component to the first telecommunications device.

Claim 29 (previously presented): A method for handling encrypted user data objects as claimed in claim 25, wherein the rights object is transmitted by the data provisioning component to the first telecommunications device if compatibility has been established based on an agreement of the checksums of the confirmation object assigned to the rights object and the encrypted user data object transmitted to the first telecommunications device in the container object.

Claim 30 (previously presented): A method for handling encrypted user data objects as claimed in claim 25, wherein following a successful comparison of the extracted checksum with the re-determined checksum, the method further comprises:

requesting description information relating to the content of the encrypted user data object from the data provisioning component;

transmitting the requested description information from the data provisioning component to the first telecommunications device; and checking whether the content having the attributes specified in the description information can be used by the first telecommunications device.

Claim 31 (previously presented): A method for handling encrypted user data objects, the method comprising:

providing an encrypted user data object in a first telecommunications device;

requesting description information relating to content of the encrypted user data object from a data provisioning component;

transmitting the requested description information from the data provisioning component to the first telecommunications device;

checking whether the content having the attributes specified in the description information can be used by the first telecommunications device; and

requesting from the data provisioning component, upon successful checking of the attributes specified in the description information, a confirmation object which is assigned to a rights object assigned to the encrypted user data object in order to check compatibility of the rights object and the encrypted user data object.

Claim 32 (previously presented): A method for handling encrypted user data objects as claimed in claim 31, wherein the rights object is transmitted by the data provisioning component to the first telecommunications device upon successful checking of the compatibility of the rights object and the encrypted user data object.

Claim 33 (previously presented): A method for handling encrypted user data objects as claimed in claim 31, wherein the encrypted user data object is provided in a content section of a container object.

Claim 34 (previously presented): A method for handling encrypted user data objects as claimed in claim 33, wherein the container object further includes a description section in which a checksum of the encrypted user data object is provided.

Claim 35 (previously presented): A method for handling encrypted user data objects as claimed in claim 34, wherein an address of the data provisioning component is also provided in the description section of the container object for purposes of requesting at least one of the description information and the confirmation object.

Claim 36 (previously presented): A method for handling encrypted user data objects as claimed in claim 34, wherein the confirmation object has a checksum of the encrypted user data object, the compatibility of the rights object and the encrypted user data object being checked, the checking comprising:

extracting the checksum from the confirmation object; and

comparing the checksum extracted from the confirmation object with the checksum provided in the description section of the container object so that, should the two checksums tally, the compatibility of the rights object assigned to the confirmation object and the encrypted user data object provided in the container object transmitted to the first telecommunications device may be concluded.

Claim 37 (previously presented): A method for handling encrypted user data objects as claimed in claim 25, wherein at least one of:

a first confirmation message is sent by the first telecommunications device to the data provisioning component if the compatibility of the rights object assigned to the confirmation object and the encrypted user data object transmitted to the first telecommunications device in the container object has been established; and

a second confirmation message is sent if the first telecommunications device has received the rights object from the data provisioning component.

Claim 38 (previously presented): A method for handling encrypted user data objects as claimed in claim 28, further comprising transmitting charging information relating to the transmitted rights object to a telecommunications subscriber assigned to the first telecommunications device.

Claim 39 (previously presented): A method for handling encrypted user data objects as claimed in claim 25, wherein the checksum is a hash value calculated according to a hash algorithm.

Claim 40 (previously presented): A method for handling encrypted user data objects as claimed in claim 27, wherein at least one of the first telecommunications device and the at least one further telecommunications device are part of a first telecommunications mobile radio network.

Claim 41 (previously presented): A method for handling encrypted user data objects as claimed in claim 25, wherein the data provisioning component is part of a second telecommunications network.

Claim 42 (previously presented): A method for handling encrypted user data objects as claimed in claim 27, wherein at least one of the first telecommunications device and the at least one further telecommunications device include a radio module.

Claim 43 (previously presented): A method for handling encrypted user data objects as claimed in claim 42, wherein the radio module is one of a mobile phone, a cordless telephone and a portable computer.

Claim 44 (previously presented): A method for handling encrypted user data objects as claimed in claim 27, wherein data is transmitted between the first telecommunications device and the at least one further telecommunications device via WAP protocols.

Claim 45 (previously presented): A method for handling encrypted user data objects as claimed in claim 27, wherein data is transmitted between the first telecommunications device and the at least one further telecommunications device via Internet protocols.

Claim 46 (previously presented): A method for handling encrypted user data objects as claimed in claim 45, wherein the Internet protocol is Hypertext Transfer protocol.

Claim 47 (previously presented): A method for handling encrypted user data objects as claimed in claim 25, wherein the user data objects include at least one of text information, audio information, video information, executable programs and software modules.

Claim 48 (previously presented): A telecommunications system for handling encrypted user data objects, comprising:

a data provisioning system having at least one data provisioning component;

and

at least one first telecommunications device;

wherein a rights object is generated for an encrypted user data object by the data provisioning component, the rights object having assignment information for assigning the rights object to a container object having an encrypted user data object, decryption information for decrypting the encrypted user data object, and rights information for describing usage rights of the encrypted user data object;

wherein a confirmation object assigned to the rights object is generated by the data provisioning component, the confirmation object having assignment information for assigning the rights object to an encrypted user data object and the checksum of the encrypted user data object;

wherein a container object is transmitted to the first telecommunications device, the container object having a content section in which an encrypted user data object is provided,

and a description section in which a determined checksum of the encrypted user data object is provided;

wherein the checksum is extracted from the description section of the container object;

wherein the checksum of the encrypted user data object provided in the content section of the container object is re-determined;

wherein the extracted checksum is compared with the re-determined checksum so that, should the two checksums tally, an error-free transmission of the encrypted user data object may be concluded;

wherein the first telecommunication device requests the confirmation object assigned to the rights object to be transmitted to the first telecommunications device;

wherein the confirmation object is transmitted from the data provisioning component to the first telecommunications device;

wherein the checksum from the confirmation object is extracted; and

wherein the checksum extracted from the confirmation object is compared with the re-determined checksum so that, should the two checksums tally, compatibility of the rights object assigned to the confirmation object and the encrypted user data object transmitted to the first telecommunications device in the container object may be concluded.